UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/034,367 | 12/27/2001 | Fabio R. Maino | ANDIP004/425452 | 8712 |

22434 7590 10/08/2010

Weaver Austin Villeneuve & Sampson LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

| EXAMINER | |
|---|---|
| TESLOVICH, TAMARA | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2437 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 10/08/2010 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO@wavsip.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/034,367 | MAINO ET AL. | |
| | Examiner | Art Unit | |
| | Tamara Teslovich | 2437 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *15 July 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) *1-25* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *26-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

# DETAILED ACTION

This Office Action is in response to Applicant's remarks and amendments filed July 15, 2010.

Claims 1-25 remain withdrawn.

Claims 49-50 remain cancelled.

Claims 26-48 are pending and herein considered.

## ***Response to Arguments***

Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

## ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**Claims 26-48** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application Publication No. 2002/0129246 A1 to Blumenau et al. and further in view of United States Patent No. 6108583 to Schneck et al.

As per **claim 26**, Blumenau teaches a method for processing frames in a fibre channel network having a first network entity and a second network entity, the method comprising:

receiving a first frame at the first network entity from the second network entity in the fibre channel network, wherein the first frame is associated with a fabric login (FLOGI) or port login (PLOGI) message (pars 68-70, 157);

identifying a security enable parameter in the first frame, wherein the security enable parameter is used by the second network entity, when the second network entity is added to the fibre channel network, to determine if the first network entity has authentication capability (par 205 “Exchange IDs”);

transmitting an acknowledgement to the second network entity that the first network entity has authentication capability (par 205 “Exchange IDs”);

receiving a second frame at the first network entity from the second network entity (pars 64-68);

identifying a security control indicator in the second frame from the second network entity, wherein the security control indicator is used to determine if the second frame authenticated (par 205 “Exchange IDs”).

Blumenau fails to specifically teach wherein the security enable parameter is used to determine if the first network entity supports other security functions and whereby the acknowledgement transmitted to the second network entity includes algorithm information and a salt parameter. Blumenau also fails to specifically teach whereby the security control indicator in the second frame is used to determine if the second frame is encrypted and determining at the first

network entity that a security association identifier associated with the second frame corresponds to an entry in the security database and decrypting a first portion of the second frame by using algorithm information contained in the security database.

Schneck discloses a system and method for data communication with adaptive security in which a send host transmits a data stream to a receive host in a packet which contains an authentication data block with an authentication header which advantageously contains various fields including a verification type, a security algorithm, a minimum security level, a target security level and an actual security level (abstract). This security enable parameter is used to determine if the first network entity supports authentication and other security functions and is included as part of the "initial training procedure" disclosed in column 8 lines 19-24 wherein the desired security parameters are communicated from the send host to the receive host where they are evaluated in order to determine whether or not receive host has the necessary capabilities or whether the actual security configuration need be altered (col.8 lines 23-40). The communication of security algorithms and salt parameters is also clearly disclosed in column 4 lines 33-50, col.8 lines 1-5 and throughout the Schneck reference. Schneck teaches whereby the security control indicator in the second frame is used to determine if the second frame is encrypted and determining at the first network entity that a security association identifier associated with the second frame corresponds to an entry in the security database and decrypting a

first portion of the second frame by using algorithm information contained in the security database (col.5 lines 33-45; col.11 lines 53-67; col.12 lines 35-41).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Blumenau the security capabilities described in Scheck, including but not limited to the transmission of algorithm and salt information as well as the use of security association identifiers and associated security database entries in order to facilitate secure fibre communications.

As per **claim 27**, the combined method of Blumenau and Schneck teaches wherein the entry in the security database was created after a fibre channel network authentication sequence between the first and second network entities (Schneck col. 8 lines 19-24 "initial training procedure").

As per **claim 28**, the combined method of Blumenau and Schneck teaches wherein the first portion is decrypted using a key contained in the entry in the security database (Blumenau par 198; Schneck col.4 lines 33-42).

As per **claim 29**, the combined method of Blumenau and Schneck teaches wherein the first portion is encrypted using DES, 3DES or AES (Schneck col.4 lines 42-50).

As per **claim 30**, the combined method of Blumenau and Schneck teaches recognizing that a second portion of the second frame supports authentication; using algorithm information contained in the entry in the security database to authenticate the second portion of the second frame (Blumenau par 205 “Exchange IDs”).

As per **claim 31**, the combined method of Blumenau and Schneck teaches wherein the second portion is authenticated using MD5 or SHA1 (Schneck col.4 lines 42-50).

As per **claim 32**, the combined method of Blumenau and Schneck teaches wherein the authentication sequence is a fibre channel login sequence between the first and second network entities (Blumenau pars 68-70, 157).

As per **claim 33,** the combined method of Blumenau and Schneck teaches wherein the login sequence is a PLOGI or FLOGI sequence (Blumenau pars 68-70, 157).

As per **claim 34**, the combined method of Blumenau and Schneck teaches wherein the first and second network entities are domain controllers and the authentication sequence is a FC-CT sequence (Blumenau pars 68-70, 157).

As per **claim 35**, the combined method of Blumenau and Schneck teaches wherein the first and second network entities are domain controllers and the authentication sequence is a SW-TL sequence (Blumenau pars 68-70, 157).

As per **claim 36**, Blumenau teaches a method for transmitting encrypted frames in a fibre channel network having a first network entity and a second network entity, the method comprising:

transmitting a first fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity, the first fibre channel including a security enable indicator, wherein the first fibre channel frame is associated with a fabric login (FLOGI) or port login (PLOGI) message (pars 68-70, 157), wherein the security enable parameter is used by the first network entity, when the first network entity is added to the fibre channel network, to determine if the second network entity has authentication capability (par 205 “Exchange IDs”);

receiving an acknowledgement from the second network entity indicating that the second network entity has authentication capability (par 205 “Exchange IDs”);

identifying a second fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity (pars 64-68);

providing a security control indicator in the second fibre channel frame, wherein the security control indicator is used to determine if the second frame is authenticated (par 205 “Exchange IDs”) and

transmitting the second fibre channel frame to the second network entity (par 66-67).

Blumenau fails to specifically teach wherein the security enable parameter is used to determine if the second network entity supports other security functions and whereby the acknowledgement received from the second network entity includes algorithm information and a salt parameter. Blumenau also fails to specifically teach inserting key and algorithm information from the second network entity into a security database and determining if the second fibre channel frame corresponds to the selectors of an entry in a security database in order to encrypt a first portion of the second fibre channel frame using key and algorithm information associated with the entry in the security database.

Schneck discloses a system and method for data communication with adaptive security in which a send host transmits a data stream to a receive host in a packet which contains an authentication data block with an authentication header which advantageously contains various fields including a verification type, a security algorithm, a minimum security level, a target security level and an actual security level (abstract). This security enable parameter is used to determine if the second network entity supports authentication and other security functions and is included as part of the "initial training procedure" disclosed in column 8 lines 19-24 wherein the desired security parameters are communicated

from the send host to the receive host where they are evaluated in order to determine whether or not receive host has the necessary capabilities or whether the actual security configuration need be altered (col.8 lines 23-40). The communication and use of security algorithms and salt parameters is also clearly disclosed in column 4 lines 33-50, col.8 lines 1-5 and throughout the Schneck reference. Schneck teaches whereby the security control indicator in the second frame is used to determine if the second frame is encrypted and encrypting a first portion of the second fibre channel frame using key and algorithm information associated with the entry in the security database (col.5 lines 33-45; col.11 lines 53-67; col.12 lines 35-41).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Blumenau the security capabilities described in Scheck, including but not limited to the transmission of algorithm and salt information as well as the use of security association identifiers and associated security database entries in order to facilitate secure fibre communications.

As per **claim 37**, the combined method of Blumenau and Schneck teaches wherein the entry in the security database was created after a fibre channel network authentication sequence between the first and second network entities (Schneck col. 8 lines 19-24 "initial training procedure").

As per **claim 38**, the combined method of Blumenau and Schneck teaches wherein the payload is encapsulated using the Authentication Header protocol or the Encapsulating Security Payload protocol (Schneck col.4 lines 33-42).

As per **claim 39**, the combined method of Blumenau and Schneck teaches adding security information to the header of the second fibre channel frame (Schneck col.6 lines 39-48).

As per **claim 40**, the combined method of Blumenau and Schneck teaches wherein a first portion of the fibre channel frame is encrypted using DES, 3DES, or AES (Schneck col.4 lines 42-50).

As per **claim 41**, the combined method of Blumenau and Schneck teaches wherein parameters in the header are normalized prior to encrypting the first portion of the second fibre channel frame (Blumenau pars 42, 61-62).

As per **claim 42**, the combined method of Blumenau and Schneck teaches wherein the payload is padded prior to encrypting the first portion of the fibre channel frame (Blumenau pars 42, 61-62).

As per **claim 43**, the combined method of Blumenau and Schneck teaches computing authentication data using key and algorithm information as

well as a second portion of the second fibre channel frame (Blumenau par 205 “Exchange IDs”).

As per **claim 44**, the combined method of Blumenau and Schneck teaches wherein authentication data is computed using MD5 or SHA1 (Schneck col.4 lines 42-50).

As per **claim 45,** the combined method of Blumenau and Schneck teaches wherein the authentication sequence is a fibre channel login sequence between the first and second network entities (Blumenau pars 68-70, 157).

As per **claim 46,** the combined method of Blumenau and Schneck teaches wherein the login sequence is a PLOGI or FLOGI sequence (Blumenau pars 68-70, 157).

As per **claim 47**, the combined method of Blumenau and Schneck teaches wherein the first and second network entities are domain controllers and the authentication sequence is a FC-CT sequence or an SW-ILS message (Blumenau pars 68-70, 157).

**Claim 48** corresponds to an apparatus employing the method described in claim 36 and is rejected accordingly.

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571)272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437